



Sri Lanka Institute of Information Technology

Individual Assignment

IE2062 – Web Security

Submitted by:

Student Registration Number	Student Name
IT19187488	Y.K.Lumindu Dilumka

Link to the video-

<https://mysliit.sharepoint.com/sites/WSAssignment874/Shared%20Documents/General/Final%20Video/IT19187488.mp4>

Objective

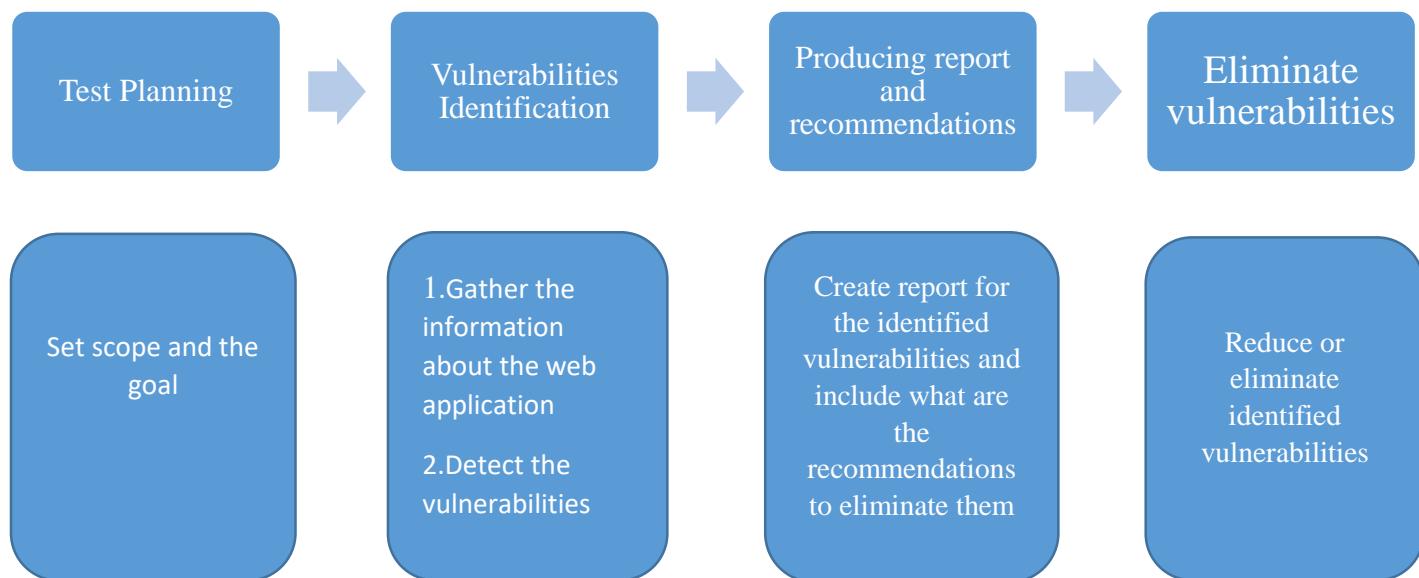
The aim of this evaluation is to define web application vulnerabilities and to show the resulting degree of risk associated with the vulnerabilities.

Application Credentials and URL

https://hackerone.com/playstation?type=team&view_policy=true

Methodology

In order to uncover the broad variety of flaws, a blended approach is adopted to conduct the evaluation that is a mixture of methods. In addition, the evaluation is adaptive in the sense of nature helps them to monitor the appraisal technique to concentrate on the sensitive areas of the program in compliance with the application features. The attack vectors are managed according to the needs of the evaluation and the selection of the attack ensures optimum application coverage.



This is the website which I'm going to use for the web audit assignment. They clearly display the bounty systems which they provide for the researchers and also there are policies that we should allowed to do when we are doing the web audit.

The screenshot shows the PlayStation bug bounty program page on the hackerone platform. At the top, there's a navigation bar with links like 'SOLUTIONS', 'PRODUCTS', 'WHY HACKERONE', 'COMPANY', 'RESOURCES', 'CONTACT US', 'START HACKING', and 'LOG IN'. Below the navigation, there's a section for PlayStation featuring their logo and a brief description: 'Recognized as a global leader in interactive and digital entertainment, Sony Interactive Entertainment (SIE) is responsible for the PlayStation brand.' A 'Submit report' button is visible. To the right, there's a 'Bug Bounty Program' section with the text 'Launched on Jun 2020' and 'Managed by HackerOne'. Below this, there's a summary of metrics: 'Reports resolved: 126', 'Assets in scope: 12', and 'Average bounty: \$400'. At the bottom of the main content area, there are tabs for 'Policy', 'Hacktivity', 'Thanks', and 'Updates (0)'. The bottom of the screen shows a taskbar with various icons and the date '2020-09-24'.

The screenshot shows the PlayStation Bug Bounty Program policy page on the hackerone.com website. The page is titled "Policy" and contains sections for "Program Overview", "Scope", "Out-of-Scope", and "Responsible Disclosure". To the right of the main content, there is a sidebar with various statistics:

Stat	Value
Total bounties paid	\$275,500
Average bounty	\$400
Top bounty range	\$1,200 - \$70,000
Bounties paid in the last 90 days	\$101,600
Reports received in the last 90 days	1723
Last report resolved	5 days ago
Reports resolved	126
Hackers thanked	103

At the bottom of the page, there is a "Scope" section listing domains that are in scope for the bounty program.

Scope

The screenshot shows the "Scopes" table from the PlayStation bug bounty program. The table lists various domains and their status regarding the bounty program:

Scope Type	Domain	Critical	Eligible
In Scope	*.playstation.net	Critical	Eligible
In Scope	*.sonyentertainmentnetwork.com	Critical	Eligible
In Scope	*.api.playstation.com	Critical	Eligible
In Scope	my.playstation.com	Critical	Eligible
In Scope	store.playstation.com	Critical	Eligible
In Scope	social.playstation.com	Critical	Eligible
In Scope	transact.playstation.com	Critical	Eligible
In Scope	wallets.api.playstation.com	Critical	Eligible
In Scope	direct.playstation.com	Critical	Eligible

First of all im going to do some recon using linux tools to get a better understanding about the domain. The first recon tool which im going to use is nikto. It can find details about Ip, Port, the start time, server and lot of other details.

```

Kali-Linux-2020.1-vmware-amd64 - VMware Workstation 15 Player (Non-commercial use only)
Player | ||| Kazam kali@kali: ~/Desktop kali@kali: ~ 02:59 PM
File Actions Edit View Help
> Executing "nikto -h"
Option host requires an argument
-config+      Use this config file
--Display+    Turn on/off display outputs
--check+     Checks files and other key files for syntax errors
--Format+    Format file (c, f, o, r, t)
--Help+      Extended help information
--host+     Target host/URL
--http+     Target host/URL
--list-plugins+ List all available plugins
--output+    Write output to this file
--nosec+     Disables using SSL/TLS security checks
--Plugins+   List of plugins to run (default: ALL)
--port+     Port to use (default 80)
--quiet+    Present the raw value to all requests, format is /directory
--ssl+      Use SSL mode on port
--Tuning+    Scan tuning
--timeout+   Timeout for requests (default: 10 seconds)
--update+   Update the database of known plugins from CIRT.net
--Version+  Print plugin and database versions
--vhost+    Virtual host (For Host header)
+ requires a value

Note: This is the short help output. Use -H for full help text.

kali@kali: $ nikto -h playstation.com
- Nikto v2.1.6

+ ERROR: Invalid IP:

kali@kali: $ nikto -h playstation.com
- Nikto v2.1.6

+ Target IP: 209.200.152.198
+ Target Hostname: playstation.com
+ Target Port: 80
+ Start Time: 2020-09-23 14:54:26 (GMT-4)

+ Server: Apache
+ The X-Content-Type-Options header is not defined. This header can hint to the user agent to protect against some forms of XSS
+ The Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type
+ Root page redirects to: https://www.playstation.com
+ Retrieved connection header: Close
+ Uncommon header 'connection' found, with contents: Close
+ No CGI Directories found. Use "all" to force check all possible dirs
+ Retrieved serverid header: web02
+ Uncommon header 'serverid' found, with contents: web02
+ Retrieved via header: MI.FRA2: 100

```

And also there's a tool called sublist3r which will search subdomains below in these search engines and details about SSL certificates to gives a better idea about the domain.

```

Kali-Linux-2020.1-vmware-amd64 - VMware Workstation 15 Player (Non-commercial use only)
Player | ||| Kazam kali@kali: ~/tools/Sublis... kali@kali: ~/tools/Sublis... Sublist3r - File Manager kali@kali: ~/tools/Sublist3r 03:12 PM
File Actions Edit View Help
kali@kali: ~/tools/Sublist3r$ python sublist3r.py -d playstation.com

Sublist3r
# Coded By Ahmed About-ElA - Gaboulsla

[-] Enumerating subdomains now for playstation.com
[-] Searching now in Baidu..
[-] Searching now in Yahoo..
[-] Searching now in Google..
[-] Searching now in Bing..
[-] Searching now in Ask..
[-] Searching now in Netcraft..
[-] Searching now in Shodan..
[-] Searching now in VirusTotal..
[-] Searching now in ThreatCrowd..
[-] Searching now in SSL Certificates..
[-] Searching now in PassiveDNS..

```

After the scan you can see more than thousands of unique subdomains are listed in playstation.com.

```

# Coded By Ahmed Aboul-Ela - @abeutu3la
[-] Enumerating subdomains now for playstation.com
[-] Searching now in Baidu..
[-] Searching now in Yahoo..
[-] Searching now in Google..
[-] Searching now in Bing..
[-] Searching now in Ask..
[-] Searching now in Netcraft..
[-] Searching now in Shodan..
[-] Searching now in VirusTotal..
[-] Searching now in ThreatCrowd..
[-] Searching now in SSL Certificates..
[-] Searching now in Whois..
[-] Total Unique Subdomains Found: 1036
www.playstation.com
account.playstation.com
metrics.playstation.com
smetrics.aem.playstation.com
antman.playstation.com
qa.playstation.com
dev.antman.playstation.com
qa.antman.playstation.com
fast.playstation.com
api.playstation.com
ai-np.api.playstation.com
accounts.api.playstation.com
www.laco.accounts.playstation.com
laco.accounts.api.playstation.com
www.laco.accounts.api.playstation.com
tip.tip.accounts.api.playstation.com
ltip-origin-lvb.accounts.api.playstation.com
ltip-origin-lvp.accounts.api.playstation.com
laco.events.laco.events.playstation.com
www.laco.events.auth.api.playstation.com
store.auth.api.playstation.com
c1-np.c1-np.api.playstation.com
core-catalog.c1-np.api.playstation.com
drift.c1-np.api.playstation.com
c1-pmgt.c1-pmgt.api.playstation.com
c1-qqa.c1-qqa.api.playstation.com
wallets.c1-qqa.api.playstation.com
c1-spint.c1-spint.api.playstation.com

```

1. I'm going to use **my.playstation.com** to find vulnerabilities using few tools.

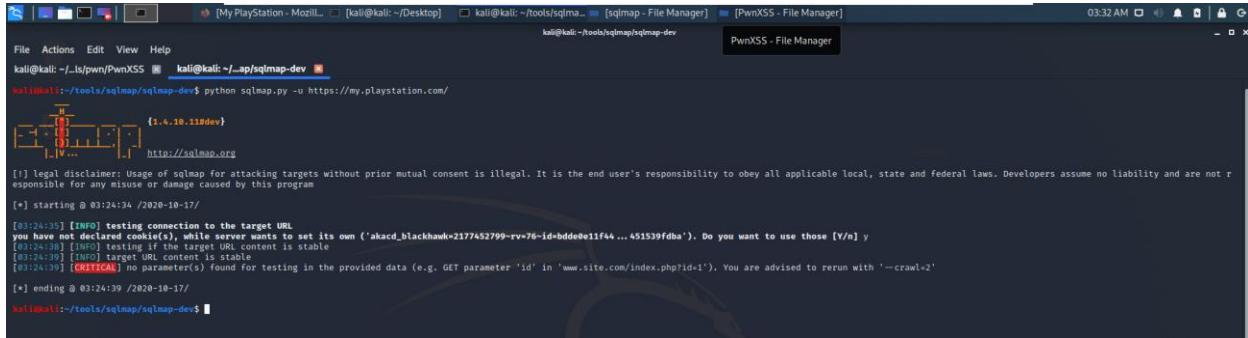
I did a pwnXSS scan to find some XSS vulnerabilities. But there was no issues with XSS vulnerabilities.

```

[03:23:15] [INFO] Checking connection to: my.playstation.com
[03:23:15] [WARNING] Internal error: Invalid URL 'my.playstation.com': No schema supplied. Perhaps you meant http://my.playstation.com?
Traceback (most recent call last):
  file "pwnXSS.py", line 73, in <module>
    start()
  file "pwnXSS.py", line 54, in start
    crawler = crawler(getopt.getopt(depth).getopt_proxy, getopt.user_agent, check(getopt), getopt.method, getopt.cookie)
  file "/home/kali/tools/pwnXSS/lib/crawler/crawler.py", line 44, in crawl
    url = self.getLinks(base, proxy, headers, cookie)
  file "/home/kali/tools/pwnXSS/lib/crawler/crawler.py", line 19, in getLinks
    return self._getLinks(url)
  file "/usr/lib/python3/dist-packages/requests/sessions.py", line 543, in get
    return self.request('GET', url, **kwargs)
  file "/usr/lib/python3/dist-packages/requests/sessions.py", line 516, in request
    prep = self.prepare_request(req)
  file "/usr/lib/python3/dist-packages/requests/sessions.py", line 459, in prepare_request
    hooks = merge_hooks([request_hooks, self.hooks])
  file "/usr/lib/python3/dist-packages/requests/models.py", line 314, in prepare_url
    self._url = self._url + url
  file "/usr/lib/python3/dist-packages/requests/models.py", line 388, in prepare_url
    raise MissingSchema(error)
requests.exceptions.MissingSchema: Invalid URL 'my.playstation.com': No schema supplied. Perhaps you meant http://my.playstation.com/
kali@kali:~/tools/pwn/PwnXSS$ python3 pwnXSS.py -u https://my.playstation.com/
<<<< STARTING >>>>
[03:23:42] [INFO] Starting PwnXSS ...
[03:23:42] [INFO] Checking connection to: https://my.playstation.com/
[03:23:43] [INFO] Connection established 200
kali@kali:~/tools/pwn/PwnXSS$ 

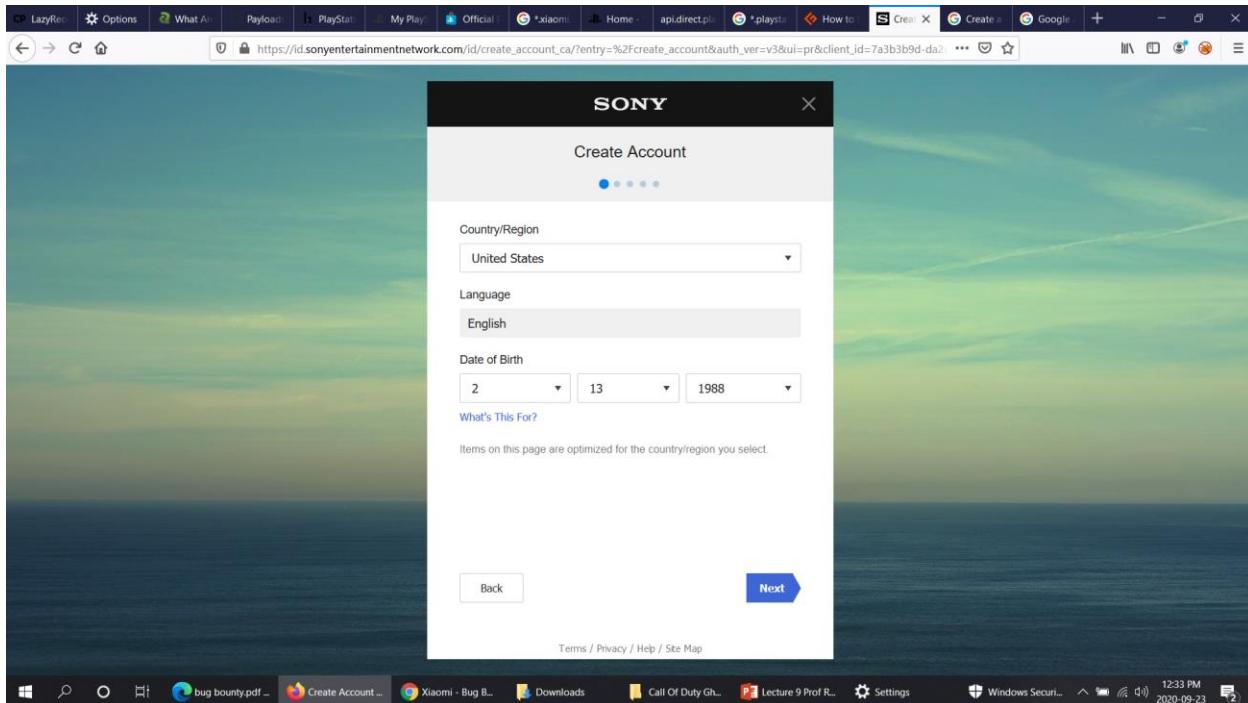
```

Then I perform a sqlmap to find whether this domain is vulnerable to sql injection flaws. After the scan I found only 1 critical vulnerability.



```
[kali@kali:~/tools/sqlmap/sqlmap-dev]$ python sqlmap.py -u https://my.playstation.com/
[*] starting @ 03:24:34 /2020-10-17/
[03:24:35] [INFO] testing connection to the target URL
you have not declared cookie(s), while server wants to set its own ('akad_blackhawk=2177452799-rv76-id=bdd0e11f44...451539fdb'). Do you want to use those [Y/n] y
[*] connection to the target URL is established
[03:24:39] [INFO] target URL content is stable
[03:24:39] [CRITICAL] no parameter(s) found for testing in the provided data (e.g. GET parameter 'id' in 'www.site.com/index.php?id=1'). You are advised to rerun with '--crawl=2'
[*] ending @ 03:24:39 /2020-10-17/
[kali@kali:~/tools/sqlmap/sqlmap-dev]$
```

I have created an account on my.playstation.com



After creating the account I just figure out what are the features can do it in this domain and I click every button to get a clear idea.

I'm also going to use burp suite to scan the vulnerabilities in my.playstation.com

The screenshot shows the Burp Suite Professional interface. The top menu bar includes 'Burp Suite Professional v2020.9 - Temporary Project - licensed to Uncia' and standard options like Project, Intruder, Repeater, Window, Help. The main window has several tabs: Dashboard, Target, Proxy, Intruder, Repeater, Sequencer, Decoder, Comparer, Extender, Project options, and User options. The 'Tasks' tab is active, showing a list of audits: '2. Live audit from Proxy (all traffic)', '3. Crawl and audit of my.playstation.com', and 'Discovering hidden content. Estimating time remaining...'. The 'Issue activity' tab is open, displaying a table of findings. The first few rows show issues related to strict transport security, such as 'Strict transport security not enforced' and 'Cacheable HTTPS response'. The 'Event log' tab is also visible, showing a list of events with filters for Critical, Error, Info, and Debug levels. The status bar at the bottom shows system information: Memory: 142.3 MB, Disk: 64.0 MB, and the date/time: 2020-10-03 7:45 PM.

After the scan you will able to see some issues are found from low to high.

This screenshot shows the 'Issues activity' tab in Burp Suite Professional. It displays a table of findings, with one row highlighted in orange. The highlighted row details an 'External service interaction (DNS)' issue found on 2020-10-13 at 20:59:30. The issue is categorized as High severity, Certain confidence, and occurs in URL path folder 2. The host is http://my.playstation.com and the path is /profile/elder-blot1/friends. The issue description explains that the application fails to prevent users from connecting to it over unencrypted connections, which can be exploited by an attacker to modify legitimate user's network traffic. The issue background notes that the payload was submitted via the HTTP Host header. The status bar at the bottom shows the date/time: 2020-10-14 11:14 AM.

Server-Side Request Forgery (SSRF)

Vulnerability title:

External Service Interaction(DNS)

Risk rating:

Severity: High

Description:

External service interaction arises when it is possible to induce an application to interact with an arbitrary external service, such as a web or mail server. The ability to trigger arbitrary external service interactions does not constitute a vulnerability in its own right, and in some cases might even be the intended behavior of the application. However, in many cases, it can indicate a vulnerability with serious consequences. The ability to send requests to other systems can allow the vulnerable server to be used as an attack proxy.

Why: Blind Amplified DNS based DDOS

How:

If a payload starting "http://..." causes a DNS-only interaction, then this strongly indicates that outbound HTTP from the server is being blocked. In this situation, a follow-up attack could target public DNS servers. Such weakness in application could be much severe with HPP where payload pushed contains multiple "https://..." values.

The screenshot shows a security audit interface with the following details:

Table of Findings:

#	T	Task	Time	Action	Issue type	Host	Path	Insertion point	Severity	Confidence	Comment
102	8		20:59:30 13 Oct 2020	Issue found	External service interaction (DNS)	http://my.playstation.com	/profile/elder-blot1/friends		High	Certain	
101	8		20:49:28 13 Oct 2020	Issue found		http://my.playstation.com	/profile/elder-blot1/friends	URL path folder 2	Information	Certain	
100	8		20:49:03 13 Oct 2020	Issue found		http://my.playstation.com	/profile/elder-blot1/friends	URL path folder 1	Information	Certain	
99	8		20:47:04 13 Oct 2020	Issue found		http://my.playstation.com	/profile/elder-blot1/friends		Information	Certain	

Detailed Request Dump:

```
GET /profile/elder-blot1/friends?98yz3ep3bd=1 HTTP/1.1
Host: 8x6e1sc011a24u1jyj0cxxxw12gge@080bxzd.burpcollaborator.net
Accept-Encoding: gzip, deflate, 98yz3ep3bd
Accept: */*, text/*;q>0.9
Accept-Language: en-US,en;q=0.9,98yz3ep3bd;q=0.9,en;q=0.9
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 Safari/537.36 98yz3ep3bd
Connection: close
Cache-Control: Max-Age=0
Origin: https://98yz3ep3bd.my.playstation.com

```

The screenshot shows a Windows desktop environment with a browser window open to a web application audit tool. The title bar reads "8. Crawl and audit of my.playstation.com". The main interface has tabs for "Details", "Audit items", "Issue activity", and "Event log". Below these are filter buttons for "Filter", "High", "Medium", "Low", "Info", "Certain", "Firm", and "Tentative". A search bar is at the top right. The central area is a table with columns: #, Task, Time, Action, Issue type, Host, Path, Insertion point, Severity, Confidence, and Comment. Several rows of audit data are listed, including entries for external service interactions and reflected inputs. A red circle highlights a specific row in the table. At the bottom of the window, there are tabs for "Advisory", "Request", "Response", and "Collaborator DNS interaction". Under "Collaborator DNS interaction", there are sections for "Description" and "DNS query". The "DNS query" section contains text about a DNS lookup received from a specific IP address on a specific date. The Windows taskbar at the bottom shows various pinned icons and the date/time "2020-10-13 9:37 PM".

Impact:

We can use the weakness as a attack proxy to DDOS all Internal/external web containers, also could be amplified too.

Mitigate threat:

- Review source code for functions such as dns.resolve(), dns.query() etc.
- Use whitelist check, boundary based validation and sanitization
- Maintain whitelist at network and web front

When scanning my.playstation.com using nikto there are some issues regarding the headers. Also there have to be some missing important headers that should include.

```

File Actions Edit View Help
kali㉿kali:~$ nikto -host my.playstation.com
- Nikto v2.1.6
+ Target IP: 184.84.52.77
+ Target Hostname: my.playstation.com
+ Target Port: 80
+ Start Time: 2020-10-14 06:57:18 (GMT-4)

+ Server: AkamaiGHost
+ Cookie akacd_blackhawk created without the httponly flag
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type
+ Root page / redirects to: https://my.playstation.com/
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ 7863 requests: 0 error(s) and 3 item(s) reported on remote host
+ End Time: 2020-10-14 07:19:57 (GMT-4) (1359 seconds)

+ 1 host(s) tested
kali㉿kali:~$ 

```

These are the missing headers that should include(Source- <https://securityheaders.com/>)

Missing Headers

Content-Security-Policy	Content Security Policy is an effective measure to protect your site from XSS attacks. By whitelisting sources of approved content, you can prevent the browser from loading malicious assets.
X-Content-Type-Options	X-Content-Type-Options stops a browser from trying to MIME-sniff the content type and forces it to stick with the declared content-type. The only valid value for this header is "X-Content-Type-Options: nosniff".
Referrer-Policy	Referrer Policy is a new header that allows a site to control how much information the browser includes with navigations away from a document and should be set by all sites.
Permissions-Policy	Permissions Policy is a new header that allows a site to control which features and APIs can be used in the browser.

2. The second domain which I scanned is <https://direct.playstation.com/en-us>

Here are the results using recon tools,

```

File Actions Edit View Help
/home/kali/tools/lazyrecon/my.playstation.com/recon-2020-10-14/my.playstation.com.txt
kali㉿kali:~$ kau@kau: ~
kali㉿kali:~$ nikto -h direct.playstation.com
- Nikto v2.1.6
+ Target IP: 125.214.166.32
+ Target Hostname: direct.playstation.com
+ Target Port: 80
+ Message: Multiple IP addresses found: 125.214.166.32, 125.214.166.27
+ Start Time: 2020-10-15 01:09:38 (GMT-4)

+ Server: AkamaiGHost
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type
+ Root page / redirects to: https://direct.playstation.com/
+ All CGI directories 'found', use '-C none' to test none
+ 26493 requests: 0 error(s) and 3 item(s) reported on remote host
+ End Time: 2020-10-15 03:25:20 (GMT-4) (8142 seconds)

+ 1 host(s) tested
kali㉿kali:~$ 

```

pwnXSS scan results,

Sq1map results,

```
Kali-Linux-2020.1-vmware-amd64 - VMware Workstation 15 Player (Non-commercial use only)
Player | Problem loading page - ... | kali@kali: ~/Desktop | kali@kali: ~/tools/sqlmap... | [sqlmap - File Manager] | [PwnXSS - File Manager] | Sublist3r - File Manager
08:06 AM 80% 🔋 🔒

File Actions Edit View Help
kali@kali: ~/tools/sqlmap/sqlmap-dev
[*] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicable local, state and federal laws. Developers assume no liability and are not responsible for any misuse or damage caused by this program
[*] starting @ 07:05:57 /2028-10-17

[07:05:58] [WARNING] you've provided target URL without any GET parameters (e.g. 'http://www.site.com/article.php?id=1') and without providing any POST parameters through option '--data'
do you want to try URL injections in the target URL itself? [Y/n] y
[*] [INFO] testing connection to the target URL
[*] [INFO] connection to target URL established ('accessdenied')
[*] [INFO] checking if the target is protected by some kind of WAF/IPS
[*] [INFO] WAF/IPS identified as 'Kona Site Defender (Akamai Technologies)'
[*] [INFO] potential permission problems detected ('Access Denied')
[*] [INFO] potential SQL injection problem detected ('Access Denied')
[*] [INFO] potential blind SQL injection problem detected ('Access Denied')
[*] [INFO] please consider usage of tamper scripts (option '--tamper')
[*] [INFO] testing if the target URL content is stable
[*] [INFO] target URL content is stable
[*] [INFO] target URL content is static
[*] [INFO] target URL content is dynamic
[*] [WARNING] URL parameter '#1' does not appear to be dynamic
[*] [WARNING] heuristic (basic) test shows that URL parameter '#1' might not be injectable
[*] [INFO] testing for SQL injection on URL parameter '#1' using 'SELECT' query
[*] [INFO] testing 'MySQL AND error-based - WHERE OR HAVING clause'
[*] [INFO] testing 'Boolean-based blind - Parameter replace (original value)'
[*] [INFO] testing 'reflective values' found and filtering out
[*] [INFO] testing 'PostgreSQL AND error-based - WHERE OR HAVING clause (FLOOR)'
[*] [INFO] testing 'Microsoft SQL Server/Sybase AND error-based - WHERE OR HAVING clause (IN)'
[*] [INFO] testing 'Oracle AND error-based - WHERE OR HAVING clause (XMLType)'
[*] [INFO] testing 'Oracle AND error-based - WHERE OR HAVING clause - Parameter replace (FLOOR)'
[*] [INFO] testing 'Generic inline queries'
[*] [INFO] testing 'PostgreSQL > 8.1 stacked queries (comment)'
[*] [CRITICAL] considerable lagging has been detected in connection response(s). Please use as high value for option '--time-sec' as possible (e.g. 10 or more)
[*] [INFO] testing 'Generic inline query - Comment'
[*] [INFO] testing 'Oracle stacked queries (DBMS_PIPE.RECEIVE_MESSAGE - Comment)'
[*] [INFO] testing 'MySQL > 5.0.12 AND time-based blind (query SLEEP)'
[*] [INFO] testing 'PostgreSQL > 8.1 AND time-based blind'
[*] [INFO] testing 'Microsoft SQL Server AND time-based blind (IF)'
[*] [INFO] testing 'Oracle AND time-based blind'
it is recommended to perform only basic UNION tests if there is not at least one other (potential) technique found. Do you want to reduce the number of requests? [Y/n] y
[*] [INFO] testing 'Generic inline query - Comment'
[*] [INFO] testing 'MySQL > 5.0.12 AND time-based blind'
[*] [CRITICAL] all tested parameters do not appear to be injectable. Try to increase values for '--level'/'--risk' options if you wish to perform more tests. If you suspect that there is some kind of protection mechanism involved (e.g. WAF) maybe you could try to use option '--tamper' (e.g. '--tamper=space2comment') and/or switch '--random-agent'
[*] [INFO] [WARNING] HTTP error codes detected during run: 400 (Forbidden) - 9 times, 404 (Not Found) - 66 times
[*] ending @ 07:58:56 /2028-10-17

kali@kali:~/tools/sqlmap/sqlmap-dev
```

This is the result after scan through burp suite and we can see some useful vulnerabilities are shown.

The screenshot shows two windows from the Burp Suite interface. The top window is a table titled '3. Crawl and audit of direct.playstation.com' with columns for #, Task, Time, Action, Issue type, Host, Path, Insertion point, Severity, Confidence, and Comment. It lists 15 vulnerabilities, including issues like input returned in response (reflected), URL path filename disclosure, and strict transport security not enforced. The bottom window is a detailed view of a TLS certificate, showing the certificate chain, issued to DigiCert Global Root CA, issued by DigiCert Global Root CA, valid from Fri Nov 05 30:00 IST 2006, and valid to Mon Nov 10 05:30:00 IST 2031. It also includes sections for issue background and references.

Encryption and Authentication

Vulnerability title:

TLS Certificate

Risk rating:

Severity: Medium

Description:

Burp relies on the Java trust store to determine whether certificates are trusted. The Java trust store does not include every root CA certificate that is included within browser trust stores. Burp might incorrectly report that a certificate is not trusted, if a valid root CA certificate is being used that is not included in the Java trust store.

TLS (or SSL) helps to protect the confidentiality and integrity of information in transit between the browser and server, and to provide authentication of the server's identity. To serve

for this purpose, the server must present an TLS certificate that is valid for the server's hostname, is issued by a trusted authority and is valid for the current date. If any one of these requirements is not met, TLS connections to the server will not provide the full protection for which TLS is designed.

It should be noted that various attacks exist against TLS in general, and in the context of HTTPS web connections in particular. It may be possible for a determined and suitably-positioned attacker to compromise TLS connections without user detection even when a valid TLS certificate is used.

Impact:

Exploits in the wild may target flaws in the TLS protocol, including weak cryptographic primitives, or specific implementation errors, cross-protocol vulnerabilities or any combination of the above.

Mitigate threat:

- Establish their security baseline with a real-time, comprehensive overview of SSL certificates and their termination endpoints across the entire network.
- Detect vulnerabilities via scanning for problematic certificates or server configurations and easily review results using Certificate Inspector's intuitive dashboard.
- Analyze security data points either by aggregate or specific to each certificate and endpoint.
- Mitigate discovered vulnerabilities, such as BEAST, and lack of compliance with industry guidelines such as the CA/Browser Forum Baseline Requirements, through recommended steps.

Vulnerability title:

Strict transport security not enforced

Risk rating:

Severity: Low

Description:

The application fails to prevent users from connecting to it over unencrypted connections. An attacker able to modify a legitimate user's network traffic could bypass the application's use of SSL/TLS encryption, and use the application as a platform for attacks against its users. This attack is performed by rewriting HTTPS links as HTTP, so that if a targeted user follows a link

to the site from an HTTP page, their browser never attempts to use an encrypted connection. The sslstrip tool automates this process.

To exploit this vulnerability, an attacker must be suitably positioned to intercept and modify the victim's network traffic. This scenario typically occurs when a client communicates with the server over an insecure connection such as public Wi-Fi, or a corporate or home network that is shared with a compromised computer. Common defenses such as switched networks are not sufficient to prevent this. An attacker situated in the user's ISP or the application's hosting infrastructure could also perform this attack. Note that an advanced adversary could potentially target any connection made over the Internet's core infrastructure.

Impact:

- User bookmarks or manually types `http://example.com` and is subject to a man-in-the-middle attacker
- HSTS automatically redirects HTTP requests to HTTPS for the target domain
- Web application that is intended to be purely HTTPS inadvertently contains HTTP links or serves content over HTTP
- A man-in-the-middle attacker attempts to intercept traffic from a victim user using an invalid certificate and hopes the user will accept the bad certificate
- HSTS does not allow a user to override the invalid certificate message

Mitigate threat:

- If the site owner would like their domain to be included in the HSTS preload list maintained by Chrome (and used by Firefox and Safari), then use the header below.
`Strict-Transport-Security: max-age=31536000; includeSubDomains; preload`
- Sending the preload directive from your site can have PERMANENT CONSEQUENCES and prevent users from accessing your site and any of its subdomains if you find you need to switch back to HTTP. Please read the details at preload removal before sending the header with preload.

These are the missing headers that should include,

Missing Headers	
Strict-Transport-Security	HTTP Strict Transport Security is an excellent feature to support on your site and strengthens your implementation of TLS by getting the User Agent to enforce the use of HTTPS. Recommended value "Strict-Transport-Security: max-age=31536000; includeSubDomains".
Content-Security-Policy	Content Security Policy is an effective measure to protect your site from XSS attacks. By whitelisting sources of approved content, you can prevent the browser from loading malicious assets.
Referrer-Policy	Referrer Policy is a new header that allows a site to control how much information the browser includes with navigations away from a document and should be set by all sites.
Permissions-Policy	Permissions Policy is a new header that allows a site to control which features and APIs can be used in the browser.

3. wallets.api.playstation.com

Here are the results using recon tools,

```
kali㉿kali:~/Desktop$ nikto -h wallets.api.playstation.com
- Nikto v2.1.6
=====
+ Target IP:          23.209.80.70
+ Target Hostname:    wallets.api.playstation.com
+ Target Port:        80
+ Start Time:         2020-10-16 04:12:32 (GMT-4)
=====
+ Server: AkamaiGHost
+ The anti-Clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type
+ All CGI directories 'found', use '-C none' to test none
```

```

kali@kali:~/tools/pwn... kali@kali:~/tools/sqlmap... [rev - File Manager] [sqlmap-dev - File Manager]
[2:20 AM 80%]

File Actions Edit View Help
kali@kali:~/tools/sqlmap/sqlmap-dev$ python3 sqlmap.py -u https://wallets.api.playstation.com/
[1.4.10.11#dev]
http://sqlmap.org

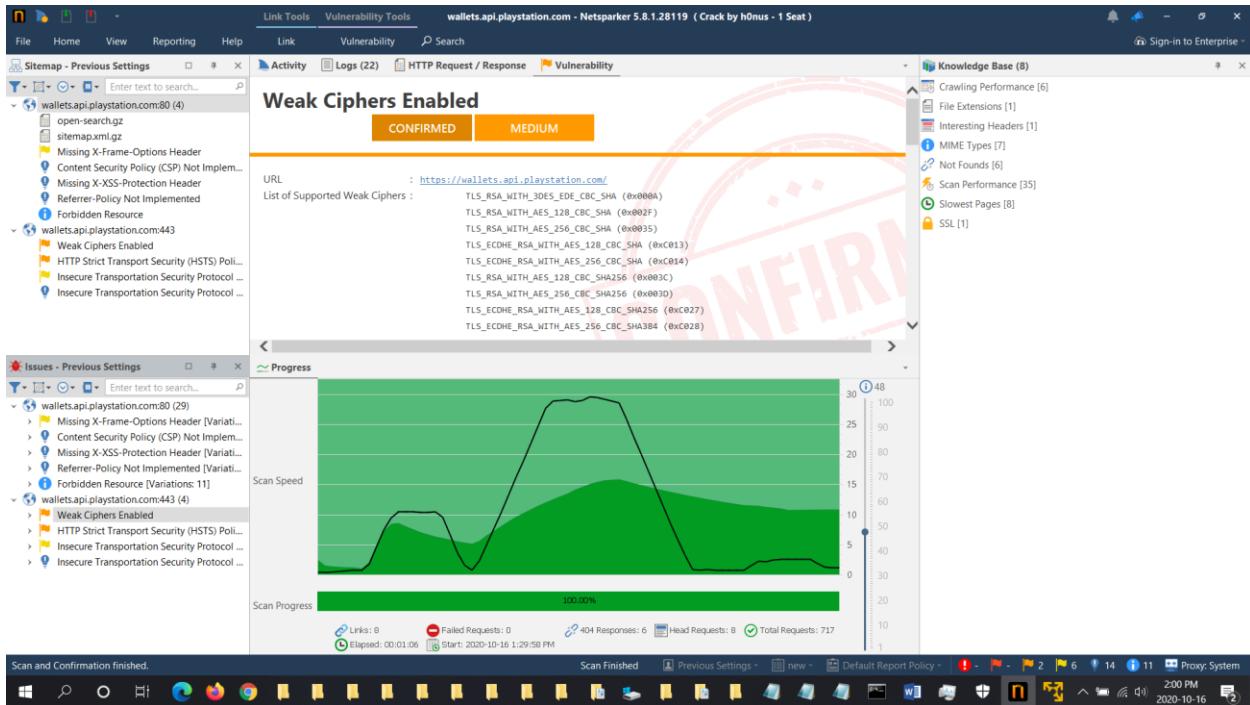
[*] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicable local, state and federal laws. Developers assume no liability and are not responsible for any misuse or damage caused by this program

[*] starting @ 02:19:50 /2020-10-20/
[*] testing connection to the target URL
[*] [WARNING] the web server responded with an HTTP error code (406) which could interfere with the results of the tests
[*] [INFO] Checking if the target is protected by some kind of NAF/IPS
[*] [INFO] [!] No NAF/IPS detected. Some SSL/TLS ciphers are still available
[*] [CRITICAL] [!] potential permission problem detected ('Access Denied')
[*] are you sure that you want to continue with further target testing? [Y/n] y
[*] [WARNING] consider usage of tamper scripts (option '--tamper')
[*] [INFO] testing if target content is stable
[*] [INFO] target URL content is stable
[*] [CRITICAL] [!] no parameter(s) found for testing in the provided data (e.g. GET parameter 'id' in 'www.site.com/index.php?id=1')
[*] [WARNING] HTTP error codes detected during run: 406 (Not Acceptable) - 2 times, 403 (Forbidden) - 1 times

[*] ending @ 02:19:55 /2020-10-20/
kali@kali:~/tools/sqlmap/sqlmap-dev$ 

```

instead of using burp I used netsparker to scan remaining domains.here are the results,



Vulnerability title:

Weak Ciphers Enabled

Risk rating:

Severity: Medium

Description:

Netsparker detected that weak ciphers are enabled during secure communication (SSL).

You should allow only strong ciphers on your web server to protect secure communication with your visitors.

Impact:

Attackers might decrypt SSL traffic between your server and your visitors.

Mitigate threat:

Configure your web server to disallow using weak ciphers

These are the missing headers that should include,

Missing Headers	
Content-Security-Policy	Content Security Policy is an effective measure to protect your site from XSS attacks. By whitelisting sources of approved content, you can prevent the browser from loading malicious assets.
X-Frame-Options	X-Frame-Options tells the browser whether you want to allow your site to be framed or not. By preventing a browser from framing your site you can defend against attacks like clickjacking. Recommended value "X-Frame-Options: SAMEORIGIN".
X-Content-Type-Options	X-Content-Type-Options stops a browser from trying to MIME-sniff the content type and forces it to stick with the declared content-type. The only valid value for this header is "X-Content-Type-Options: nosniff".
Referrer-Policy	Referrer Policy is a new header that allows a site to control how much information the browser includes with navigations away from a document and should be set by all sites.
Permissions-Policy	Permissions Policy is a new header that allows a site to control which features and APIs can be used in the browser.

4.transact.playstation.com

Here are the results using recon tools,

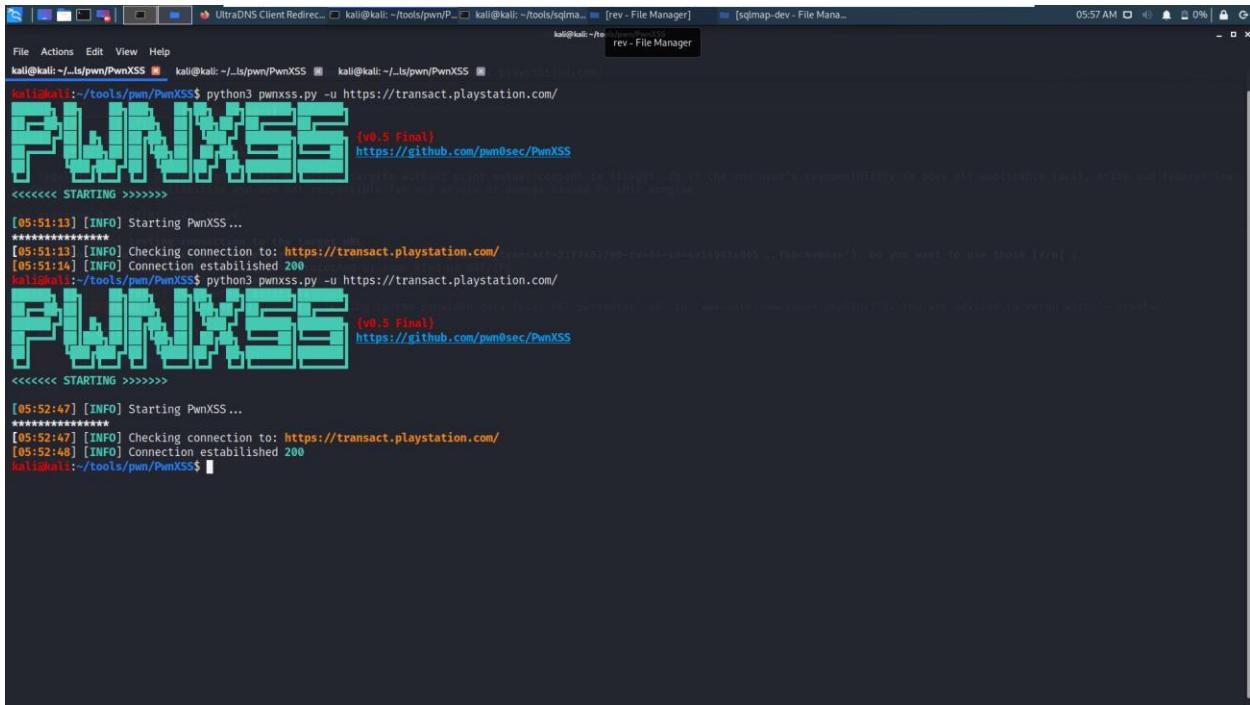
```
File Actions Edt View Help
kali㉿kali: ~/_ls/pwn/PwnXSS kali㉿kali: ~/_ls/pwn/PwnXSS kali㉿kali: ~/_ls/pwn/PwnXSS
kali㉿kali: /tools/pwn/PwnXSS nikto -h https://transact.playstation.com/
- Nikto v2.1.6

+ Target IP: 23.42.162.48
+ Target Hostname: transact.playstation.com
+ Target Port: 443

+ SSL Info: Subject: /CN=transact.playstation.com
Ciphers: TLS_AES_256_GCM_SHA384
Issuer: /C=JP/ST=Tokyo/L=Chiyoda-ku/O=Comodo Japan, Inc./CN=Comodo Japan RSA DV CA
+ Start Time: 2020-10-20 05:36:49 (GMT-4)

+ Server: AkamaiNetStorage
+ Cookie akacd_transact created without the httponly flag
+ X-Frame-Options header is set to allow framing from https://store.playstation.com/. This does not have full cross-browser support (only in IE and Firefox) and may lead to the header being ignored.
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS
+ The site uses SSL and Expect-CT header is not present.
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ Server banner has changed from 'AkamaiNetStorage' to 'AkamaiGHost' which may suggest a WAF, load balancer or proxy is in place
+ The Content-Encoding header is set to "deflate" this may mean that the server is vulnerable to the BREACH attack.
+ Storage: Try to login with 'admin' or 'monitor'
+ Uncommon header 'x-akamai-path-stats' found, with contents: [3:153202:4294967094]
/index.html.bak: The remote server (perhaps Web02) shows directory indexes if .bak is appended to the request.
/index.html.: The remote server (perhaps Web02) shows directory indexes if a ~ is appended to the request.
OSVDB-23654: /profile.php?u=jlkpk2lu: Powerboards is vulnerable to path disclosure.
OSVDB-44056: /sips/sipssys/users/a/admin/user: WebS v0.2.2 allows user account info (including password) to be retrieved remotely.
//: Appending // to a directory allows indexing
//: Apache on Red Hat Linux release 9 reveals the root directory listing by default if there is no index page.
OSVDB-122: /Fasttrack can give a directory listing if issued 'get' instead of 'GET'.
/*.*: WASD Server reveals the contents of directories with this URL. Upgrade to a later version and secure according to the documents on the WASD web site.
OSVDB-576: /*/00/: Weblogic allows directory listings with %00 (or indexing is enabled), upgrade to v6.0 SP1 or higher. http://www.securityfocus.com/bid/2513
OSVDB-576: /*ze/: Weblogic allows source code or directory listing, upgrade to v6.0 SP1 or higher. http://www.securityfocus.com/bid/2513.
OSVDB-576: /*zf/: Weblogic allows source code or directory listing, upgrade to v6.0 SP1 or higher. http://www.securityfocus.com/bid/2513.
OSVDB-576: /*sc/: Weblogic allows source code or directory listing, upgrade to v6.0 SP1 or higher. http://www.securityfocus.com/bid/2513.
OSVDB-3268: Weblogic: Directory indexing found.
/*3f.jsp: JRun 3.0 and 3.1 on IIS2000 running IIS4 or IIS5 allow directory listing by requesting %3f.jsp at the end of a URL.
/com: Java class files may be browsable.
/COM: Java class files may be browsable.
OSVDB-1210: /scripts/samples/search/fullhit.htm: Server may be vulnerable to a Webhats.dll arbitrary file retrieval. https://docs.microsoft.com/en-us/security-updates/securitybulletins/2000/MS00-006.
```

pwnXSS result,



```
kali㉿kali:~/tools/pwn/PwnXSS$ python3 pwnxss.py -u https://transact.playstation.com/
PWNXSS (v0.5 Final)
https://github.com/pwn0sec/PwnXSS

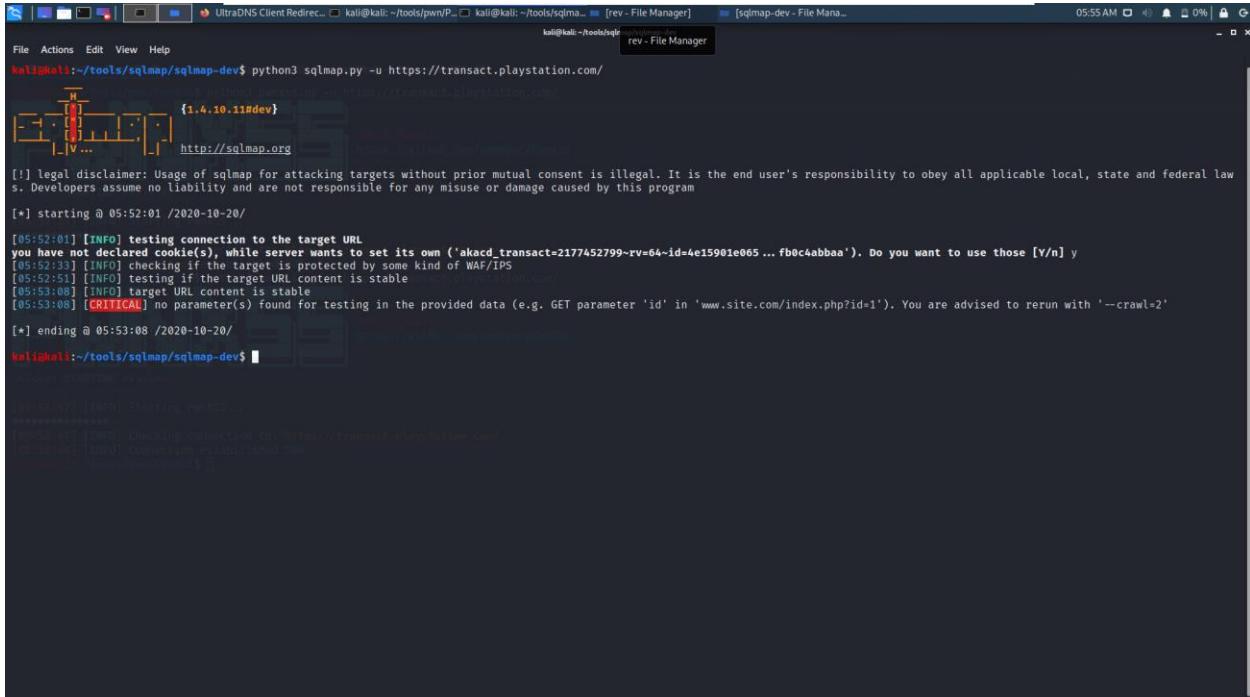
<<<<< STARTING >>>>>

[05:51:13] [INFO] Starting PwnXSS...
*****
[05:51:13] [INFO] Checking connection to: https://transact.playstation.com/
[05:51:14] [INFO] Connection established 200
kali㉿kali:~/tools/pwn/PwnXSS$ python3 pwnxss.py -u https://transact.playstation.com/
PWNXSS (v0.5 Final)
https://github.com/pwn0sec/PwnXSS

<<<<< STARTING >>>>>

[05:52:47] [INFO] Starting PwnXSS...
*****
[05:52:47] [INFO] Checking connection to: https://transact.playstation.com/
[05:52:48] [INFO] Connection established 200
kali㉿kali:~/tools/pwn/PwnXSS$
```

Sqlmap result,



```
kali㉿kali:~/tools/sqlmap/sqlmap-dev$ python3 sqlmap.py -u https://transact.playstation.com/
{ 1.4 .10 .11#dev }

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicable local, state and federal laws.
[!] Developers assume no liability and are not responsible for any misuse or damage caused by this program

[*] starting @ 05:52:01 /2020-10-20

[05:52:01] [INFO] testing connection to the target URL
you have not declared cookie(s), while server wants to set its own ('akad_transact=2177452799-rv=64~id=4e15901e065 ... fb0c4abbba'). Do you want to use those [y/n] y
[05:52:03] [INFO] checking if the target is protected by some kind of WAF/IPS
[05:52:05] [INFO] testing if the target URL content is stable
[05:53:08] [INFO] target URL content is stable
[05:53:08] [CRITICAL] no parameter(s) found for testing in the provided data (e.g. GET parameter 'id' in 'www.site.com/index.php?id=1'). You are advised to rerun with '--crawl=2'

[*] ending @ 05:53:08 /2020-10-20

kali㉿kali:~/tools/sqlmap/sqlmap-dev$
```

Vulnerability Summary

CONFIRM	VULNERABILITY	METHOD	URL	PARAMETER
	Out-of-date Version (jQuery)	GET	https://transact.playstation.com/assets/vendor-9b63638465479f9d366b0648da8bbfb.js	
	Misconfigured X-Frame-Options Header	GET	https://transact.playstation.com/opensearch.xml	
	Missing X-Frame-Options Header	GET	https://transact.playstation.com/html/webframeRedirect.html	
	Cookie Not Marked as HttpOnly	GET	http://transact.playstation.com/	
	Expect-CT Not Enabled	GET	https://transact.playstation.com/opensearch.xml	
	Missing X-XSS-Protection Header	GET	https://transact.playstation.com/opensearch.xml	
	Referrer-Policy Not Implemented	GET	https://transact.playstation.com/opensearch.xml	
	SameSite Cookie Not Implemented	GET	http://transact.playstation.com/	
	Email Address Disclosure	GET	https://transact.playstation.com/assets/psst-fe190865ca6ae935c1ae3d1c9c2217e8.js	
	Missing object-src in CSP Declaration	GET	https://transact.playstation.com/opensearch.xml	

Vulnerability title:

Out-of-date Version (jQuery)

Risk rating:

Severity: Medium

Description:

Netsparker identified the target web site is using jQuery and detected that it is out of date

```
Response
Response Time (ms) : 305.1783 Total Bytes Received : 1482770 Body Length : 1481881 Is Compressed : No

HTTP/1.1 200 OK
Transfer-Encoding: chunked
Server: AkamaiNetStorage
Expires: Sat, 16 Oct 2021 11:57:23 GMT
Vary: Accept-Encoding
Content-Security-Policy: frame-ancestors https://webstore.playstation.com https://preview.www.playstation.com https://stage.playstation.com https://my.playstation.com https://id.sonyentertainmentnetwork.com https://transact.playstation.com https://store.playstation.com https://checkout.playstation.com https://www.playstation.com https://library.playstation.com;
Connection: keep-alive
Connection: Transfer-Encoding
Last-Modified: Tue, 06 Oct 2020 19:43:06 GMT
Accept-Ranges: bytes
Strict-Transport-Security: max-age=31536000 ; includeSubDomains ; preload
Content-Type: application/x-javascript
Content-Encoding:
Date: Fri, 16 Oct 2020 11:57:23 GMT
ETag: "9b63638465479f9d366b0648da8bbffbb:1602013386.594504"
Cac
...
e,t){return t.toUpperCase()}}
function y(e){var t=!t&&"length"in e&&e.length,n=f.type(e)
return"function"!=t&&!f.isWindow(e)&&("array"==n||0==t||"number"==typeof t&&t>0&&t-1 in e)}f.fn=f.prototype={jquery:"2.2.4",constructor:f,selector:"",length:0,toArray:function(){return i.call(this)},get:function(e){return null!=e?e<0?this[e+this.length]:this[e]:i.call(this)},pushStack:function(e){var t=f.merge(this.constr
...

```

Impact:

Since this is an old version of the software, it may be vulnerable to attack

jquery Cross-Site Scripting (XSS) Vulnerability

- jQuery before 3.4.0, as used in Drupal, Backdrop CMS, and other products, mishandles `jQuery.extend(true, {}, ...)` because of `Object.prototype` pollution. If an unsanitized source object contained an enumerable `__proto__` property, it could extend the native `Object.prototype`.

These are the vulnerable security attacks for jquery version 2.2.4 according to the

https://www.cvedetails.com/vulnerability-list/vendor_id-6538/product_id-11031/version_id-286394/Jquery-Jquery-2.2.4.html

The screenshot shows the CVE Details website interface. The URL in the address bar is https://www.cvedetails.com/vulnerability-list/vendor_id-6538/product_id-11031/version_id-286394/Jquery-Jquery-2.2.4.html. The main content area displays two vulnerabilities for jQuery 2.2.4:

#	CVE ID	CWE ID	# of Exploits	Vulnerability Type(s)	Publish Date	Update Date	Score	Gained Access Level	Access	Complexity	Authentication	Conf.	Integ.	Avail.
1	CVE-2019-11358	79	XSS		2019-04-19	2019-06-12	4.3	None	Remote	Medium	Not required	None	Partial	None
2	CVE-2015-9251	79	XSS		2018-01-18	2019-06-10	4.3	None	Remote	Medium	Not required	None	Partial	None

A detailed description for the first vulnerability states: "jQuery before 3.4.0, as used in Drupal, Backdrop CMS, and other products, mishandles `jQuery.extend(true, {}, ...)` because of `Object.prototype` pollution. If an unsanitized source object contained an enumerable `__proto__` property, it could extend the native `Object.prototype`".

The bottom of the page shows a footer with various links like "Vulnerability Feeds & Widgets", "www.itsecdb.com", and a search bar.

[Home](#)

Browse :

- [Vendors](#)
- [Products](#)
- [Vulnerabilities By Date](#)
- [Vulnerabilities By Type](#)

Reports :

- [CVSS Score Report](#)
- [CVSS Score Distribution](#)

Search :

- [Vendor Search](#)
- [Product Search](#)
- [Version Search](#)
- [Vulnerability Search](#)
- [By Microsoft References](#)

Top 50 :

- [Vendors](#)
- [Vendor CVSS Scores](#)
- [Products](#)
- [Product CVSS Scores](#)
- [Versions](#)

Other :

- [Microsoft Bulletins](#)
- [Bugtraq Entries](#)
- [CWE Definitions](#)
- [About & Contact](#)

CVE Details

The ultimate security vulnerability datasource

Log In Register

(e.g.: CVE-2009-1234 or 2010-1234 or 20101234)

Vulnerability Feeds & Widgets [New](#) [www.itsecdb.com](#)

Vulnerability Details : CVE-2019-11358

jQuery before 3.4.0, as used in Drupal, Backdrop CMS, and other products, mishandles `jQuery.extend(true, {}, ...)` because of Object.prototype pollution. If an unsanitized source object contained an enumerable `__proto__` property, it could extend the native Object.prototype.

Publish Date : 2019-04-19 Last Update Date : 2019-06-12

[Collapse All](#) [Expand All](#) [Select](#) [Select&Copy](#) [Scroll To](#) [Comments](#) [External Links](#)

[Search](#) [Twitter](#) [Search YouTube](#) [Search Google](#)

- CVSS Scores & Vulnerability Types

CVSS Score	4.3
Confidentiality Impact	None (There is no impact to the confidentiality of the system.)
Integrity Impact	Partial (Modification of some system files or information is possible, but the attacker does not have control over what can be modified, or the scope of what the attacker can affect is limited.)
Availability Impact	None (There is no impact to the availability of the system.)
Access Complexity	Medium (The access conditions are somewhat specialized. Some preconditions must be satisfied to exploit)
Authentication	Not required (Authentication is not required to exploit the vulnerability.)
Gained Access	None
Vulnerability Type(s)	Cross Site Scripting
CWE ID	79

- Related OVAL Definitions

Title	Definition Id	Class	Family

Mitigate threat:

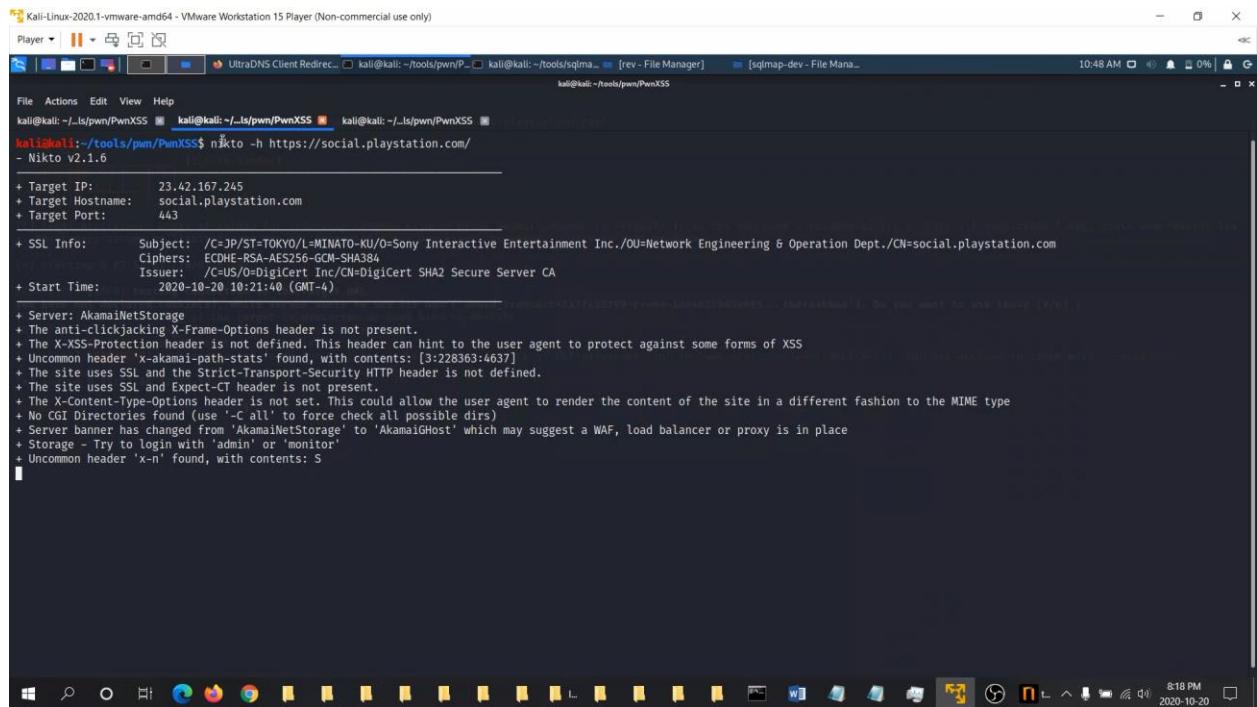
Upgrade your installation of jQuery to the latest stable version.

These are the missing headers that should include,

Missing Headers	
X-Content-Type-Options	X-Content-Type-Options stops a browser from trying to MIME-sniff the content type and forces it to stick with the declared content-type. The only valid value for this header is "X-Content-Type-Options: nosniff".
Referrer-Policy	Referrer Policy is a new header that allows a site to control how much information the browser includes with navigations away from a document and should be set by all sites.
Permissions-Policy	Permissions Policy is a new header that allows a site to control which features and APIs can be used in the browser.

5. <https://social.playstation.com/>

Here are the results using recon tools,



The screenshot shows a terminal window on a Kali Linux desktop environment. The terminal is running the Nikto web scanner against the target website. The output of the scan is displayed, detailing various findings such as SSL info, server software, and security headers. The terminal window is part of a larger desktop interface with other applications like UltraDNS Client Redirector and sqlmap-dev visible in the background.

```
kali@kali:~/tools/pwn/PwnXSS$ nikto -h https://social.playstation.com/
- Nikto v2.1.6
+ Target IP: 23.42.167.245
+ Target Hostname: social.playstation.com
+ Target Port: 443
+ SSL Info: Subject: /C=JP/ST=TOKYO/L=MINATO-KU/O=Sony Interactive Entertainment Inc./OU=Network Engineering & Operation Dept./CN=social.playstation.com
Ciphers: ECDHE-RSA-AES256-GCM-SHA384
Issuer: /C=US/O=DigiCert Inc/CN=DigiCert SHA2 Secure Server CA
+ Start Time: 2020-10-20 10:21:40 (GMT-4)
+ Server: AkamaiNetStorage
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS
+ Uncommon header 'x-akamai-path-stats' found, with contents: [3:28363:4637]
+ The site uses SSL and the Strict-Transport-Security HTTP header is not defined.
+ The site uses SSL and Expect-CT header is not present.
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ Server banner has changed from 'AkamaiNetStorage' to 'AkamaiGHost' which may suggest a WAF, load balancer or proxy is in place
+ Storage - Try to login with 'admin' or 'monitor'
+ Uncommon header 'x-n' found, with contents: S
```

```
Kali-Linux-2020.1-vmware-amd64 - VMware Workstation 15 Player (Non-commercial use only)
Player ||| & 11:03 AM 0% 09:33 PM 2020.10.20

UltraDNS Client Redirect... kali@kali: ~/tools/pwn/PwnXSS kali@kali: ~/tools/sqlmap... [rev - File Manager] [sqlmap-dev - File Mana...
File Actions Edit View Help
kali@kali: ~/ls/pwn/PwnXSS kali@kali: ~/ls/pwn/PwnXSS kali@kali: ~/ls/pwn/PwnXSS

kali@kali:~/tools/pwn/PwnXSS$ python3 pwnxss.py -u https://social.playstation.com/
PwnXSS (v0.5 Final)
https://github.com/pwn0sec/PwnXSS
<<<<< STARTING >>>>>
[11:03:00] [INFO] Starting PwnXSS...
*****
[11:03:00] [INFO] Checking connection to: https://social.playstation.com/
[11:03:01] [INFO] Connection failed 404
kali@kali:~/tools/pwn/PwnXSS$ python3 pwnxss.py -u https://social.playstation.com/
PwnXSS (v0.5 Final)
https://github.com/pwn0sec/PwnXSS
<<<<< STARTING >>>>>
[11:03:08] [INFO] Starting PwnXSS...
*****
[11:03:08] [INFO] Checking connection to: https://social.playstation.com/
[11:03:09] [INFO] Connection failed 404
kali@kali:~/tools/pwn/PwnXSS$
```

```

[+] Starting @ 11:03:21 /2020-10-20/
[11:03:21] [INFO] testing connection to the target URL
[11:03:22] [CRITICAL] page not found (404)
it is not recommended to continue in this kind of cases. Do you want to quit and make sure that everything is set up properly? [y/n] y
[11:03:27] [WARNING] HTTP error codes detected during run:
404 (Not Found) - 1 times
[*] ending @ 11:03:27 /2020-10-20/

```

After the scan using netsparker I got the same issues like in the previous domains and I have already explained about them.

Weak Ciphers Enabled

CONFIRMED | MEDIUM

URL : <https://social.playstation.com/>

List of Supported Weak Ciphers :

- TLS_RSA_WITH_3DES_EDE_CBC_SHA (0x0008)
- TLS_RSA_WITH_AES_256_CBC_SHA (0x0035)
- TLS_RSA_WITH_AES_128_CBC_SHA (0x002F)
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xC014)
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xC013)
- TLS_RSA_WITH_AES_256_ChaSHA256 (0x003D)
- TLS_RSA_WITH_AES_128_ChaSHA256 (0x003C)
- TLS_ECDHE_RSA_WITH_AES_256_ChaSHA384 (0xC028)
- TLS_ECDHE_RSA_WITH_AES_128_ChaSHA256 (0xC027)

Vulnerability Details

CLASSIFICATION

PCI DSS 3.2
OWASP 2013

Scan Speed

Scan Progress 100.00%

Links: 1 Failed Requests: 0 404 Responses: 1 Head Requests: 50 Total Requests: 338

These are the missing headers that should include,

Missing Headers	
Content-Security-Policy	Content Security Policy is an effective measure to protect your site from XSS attacks. By whitelisting sources of approved content, you can prevent the browser from loading malicious assets.
X-Frame-Options	X-Frame-Options tells the browser whether you want to allow your site to be framed or not. By preventing a browser from framing your site you can defend against attacks like clickjacking. Recommended value "X-Frame-Options: SAMEORIGIN".
X-Content-Type-Options	X-Content-Type-Options stops a browser from trying to MIME-sniff the content type and forces it to stick with the declared content-type. The only valid value for this header is "X-Content-Type-Options: nosniff".
Referrer-Policy	Referrer Policy is a new header that allows a site to control how much information the browser includes with navigations away from a document and should be set by all sites.
Permissions-Policy	Permissions Policy is a new header that allows a site to control which features and APIs can be used in the browser.

6. <https://live.playstation.com/#/>

Here are the results using recon tools,

After the scan using linux tools we cannot see any important issues here.

```
5 std::backtrace (by Raymond) / 0x0000000000410000
Player Player -||- □ [ ] 
Server Not Found - Mozilla Firefox - kali@kali: ~/tools/pwn/PwnXSS - kali@kali: ~/tools/sqlmap - kali@kali: ~/tools/Sublist3r - [rev - File Manager] - Sublist3r - File Manager
02:31 AM 0% ↻
File Actions Edit View Help
kali@kali: ~/ls/pwn/PwnXSS [kali@kali: ~/ls/pwn/PwnXSS] kali@kali: ~/ls/pwn/PwnXSS [kali@kali: ~/ls/pwn/PwnXSS]
kali@kali: ~/tools/pwn/PwnXSS$ nikto -h live.playstation.com
- Nikto v2.1.6

+ Target IP: 13.35.13.102
+ Target Hostname: live.playstation.com
+ Target Port: 80
+ Message: Multiple IP addresses found: 13.35.13.102, 13.35.13.60, 13.35.13.98, 13.35.13.47
+ Start Time: 2020-10-21 02:22:36 (GMT-4)

+ Server: CloudFront
+ Retrieved via header: 1.1 4bc700d87dc12c5b9fe83b91ddd63beb.cloudfront.net (CloudFront)
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS
+ Uncommon header 'x-amz-cf-pop' found, with contents: SIN5-C1
+ Uncommon header 'x-cache' found, with contents: Redirect from cloudfront
+ Uncommon header 'x-amz-cf-id' found, with contents: iuxsu2nclq6W9DscP0g_lbI59w9UhDJ6aYcu1LzqTLIzVXII4Iung=
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type
+ Root page / redirects to: https://live.playstation.com/
+ No CGI Directories found (use '-C all' to force check all possible dirs)
```

```
[*] Kali-Linux-2020.1-vmware-amd64 - VMware Workstation 15 Player (Non-commercial use only)
Player ▾ | || ▾ ▾ ▾
Server Not Found - Mozilla Firefox - kali@kali: ~/tools/pwn/PwnXSS - kali@kali: ~/tools/sqlmap - kali@kali: ~/tools/Sublist3r - [rev - File Manager] - Sublist3r - File Manager
03:14 AM 0% 12:43 PM 2020-10-21

File Actions Edit View Help
kali@kali: ~/tools/pwn/PwnXSS □ kali@kali: ~/tools/pwn/PwnXSS □ kali@kali: ~/tools/pwn/PwnXSS □
kali@kali: ~/tools/pwn/PwnXSS$ python3 pwnxss.py -u https://live.playstation.com/#
PWNXSS {v0.5 Final} https://github.com/pwn0sec/PwnXSS
<<<<< STARTING >>>>>
[03:13:58] [INFO] Starting PwnXSS...
*****
[03:13:58] [INFO] Checking connection to: https://live.playstation.com/#
[03:13:59] [INFO] Connection established 200
kali@kali: ~/tools/pwn/PwnXSS$
```

```

Player -> Server Not Found - Mozilla Firefox kali@kali: ~ /tools/pwn/P_ kali@kali: ~ /tools/sqlma... kali@kali: ~ /tools/Sublis... [rev - File Manager] Sublist3r - File Manager 03:14 AM 0% G
File Actions Edit View Help
kali@kali:~/tools/sqlmap/sqlmap-dev$ python3 sqlmap.py -u https://live.playstation.com/#

{ 1.4.10.11#dev }
http://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicable local, state and federal laws. Developers assume no liability and are not responsible for any misuse or damage caused by this program

[*] starting @ 03:14:22 /2020-10-21/
[03:14:22] [INFO] testing connection to the target URL
[03:14:23] [INFO] checking if the target is protected by some kind of WAF/IPS
[03:14:23] [INFO] testing if the target URL content is stable
[03:14:23] [INFO] target URL content is stable
[03:14:23] [CRITICAL] no parameter(s) found for testing in the provided data (e.g., GET parameter 'id' in 'www.site.com/index.php?id=1'). You are advised to rerun with '--crawl=2'

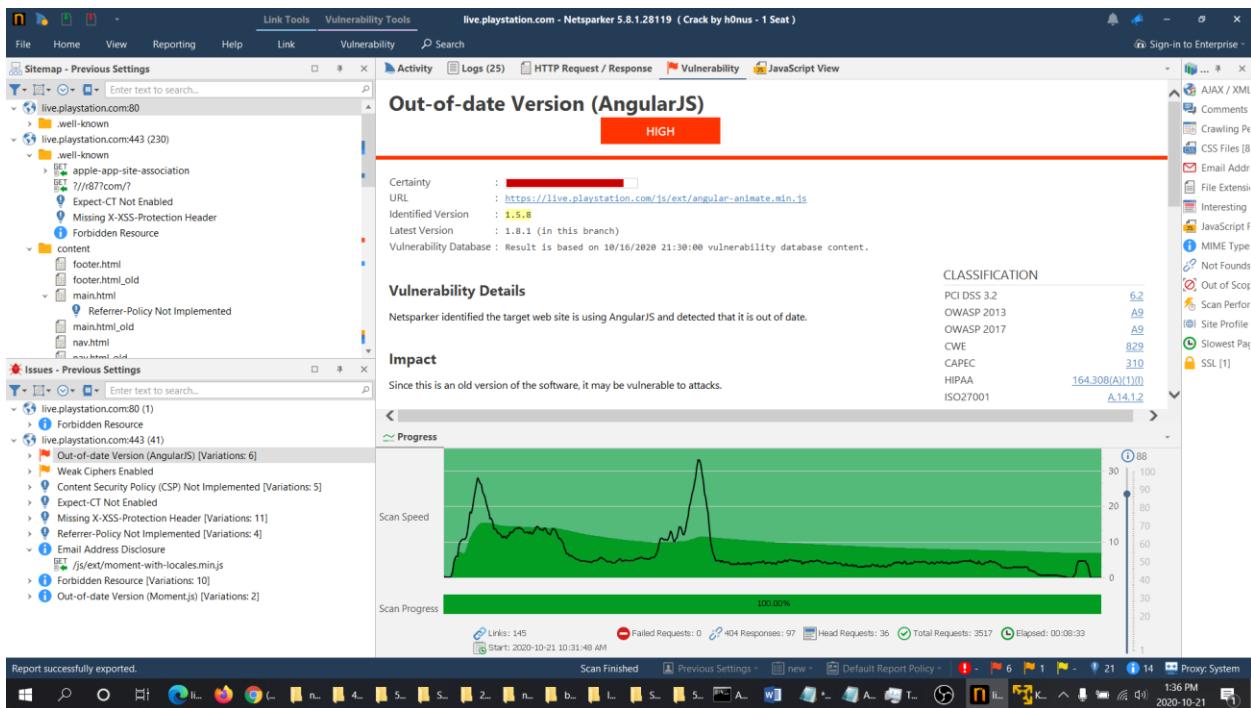
[*] ending @ 03:14:23 /2020-10-21/
kali@kali:~/tools/sqlmap/sqlmap-dev$ 

```

But netsparker able to capture some important issues after the scan.

Vulnerability Summary

CONFIRM	VULNERABILITY	METHOD	URL	PARAMETER
!	Out-of-date Version (AngularJS)	GET	https://live.playstation.com/js/ext/angular-sanitize.min.js	
!	Weak Ciphers Enabled	GET	https://live.playstation.com/	
!	Content Security Policy (CSP) Not Implemented	GET	https://live.playstation.com/	
!	Expect-CT Not Enabled	GET	https://live.playstation.com/.well-known/	
!	Missing X-XSS-Protection Header	GET	https://live.playstation.com/.well-known/	
!	Referrer-Policy Not Implemented	GET	https://live.playstation.com/content/main.html	
!	Email Address Disclosure	GET	https://live.playstation.com/js/ext/moment-with-locales.min.js	
!	Out-of-date Version (Moment.js)	GET	https://live.playstation.com/	
!	Forbidden Resource	GET	https://live.playstation.com/.well-known/	



Vulnerability title:

Out-of-date Version (AngularJS)

Risk rating:

Severity: High

Description:

Netsparker identified the target web site is using AngularJS and detected that it is out of date. This currently running in version 1.5.8.

Response

Response Time (ms) : 349.8615 Total Bytes Received : 6438 Body Length : 5861 Is Compressed : No

```
HTTP/1.1 200 OK
Server: AmazonS3
X-Cache: Hit from cloudfront
Connection: keep-alive
Via: 1.1 b95596d6887b20449c59c2fc9d141c4a.cloudfront.net (CloudFront)
Content-Length: 5861
Last-Modified: Fri, 31 Aug 2018 20:13:29 GMT
Accept-Ranges: bytes
X-Frame-Options: SAMEORIGIN
Strict-Transport-Security: max-age=63072000; includeSubdomains; preload
Content-Type: application/javascript
X-Amz-Cf-Pop: SIN5-C1
X-Amz-Cf-Id: BSf3SrKkR380syr6DZ-19PsbJ617T0fxTeoR4FHCLBDf8YnJu2c_UQ==
Age: 28198
Date: Tue, 20 Oct 2020 21:12:03 GMT
ETag: "1ed87cdd5af63f804f"
...
/javascript
X-Amz-Cf-Pop: SIN5-C1
X-Amz-Cf-Id: BSf3SrKkR380syr6DZ-19PsbJ617T0fxTeoR4FHCLBDf8YnJu2c_UQ==
Age: 28198
Date: Tue, 20 Oct 2020 21:12:03 GMT
ETag: "1ed87cdd5af63f804fb0889392dd3917"

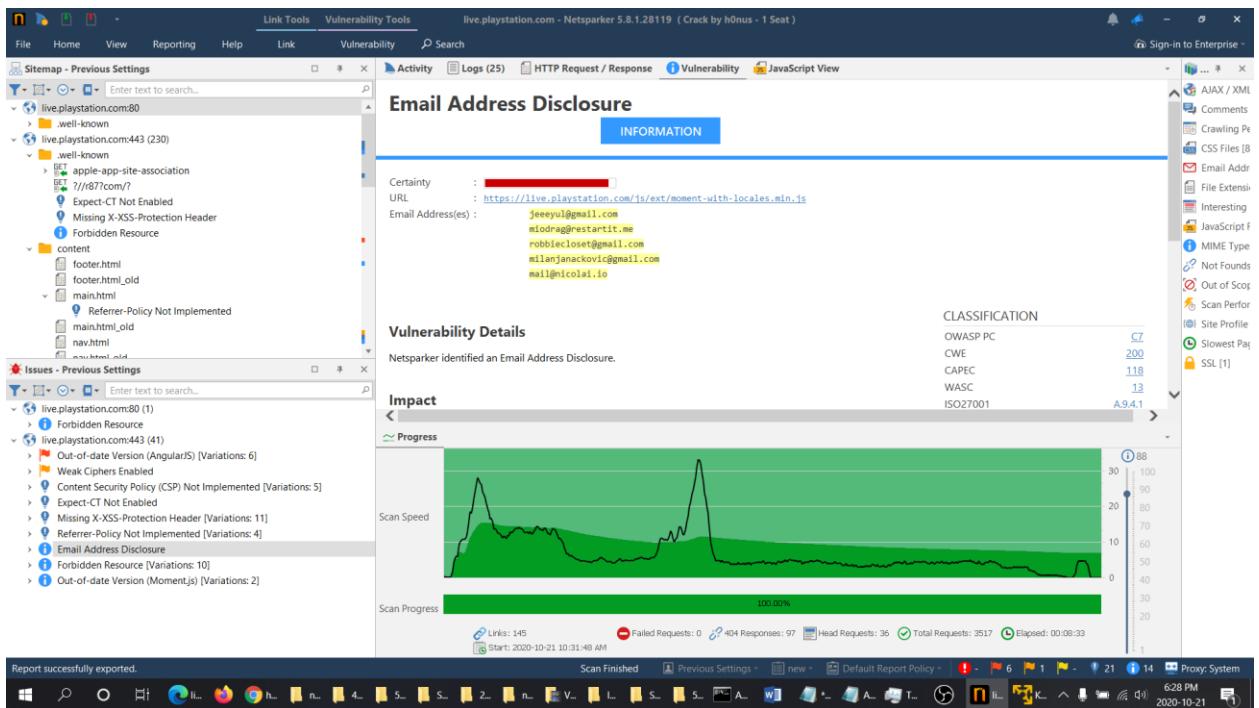
/*
AngularJS v1.5.8
(c) 2010-2016 Google, Inc. http://angularjs.org
License: MIT
*/
(function(s,g){'use strict';function H(g){var l=[];t(l,A).chars(g);return l.join("")}var B=g.$$minErr("$sanitize").C.I.D.F.a.A.F.t:p.
```

Impact:

Since this is an old version of the software, it may be vulnerable to attacks like XSS.

Mitigate threat:

The AngularJS should upgrade to the latest stable version.



Vulnerability title:

Email Address Disclosure

Risk rating:

Severity: Information

Description:

Netsparker identified an Email Address Disclosure

```

///! author : Jeeeyul Lee <jeeeyul@gmail.com>
a.defineLocale("ko", {months:"1월_2월_3월_4월_5월_6월_7월_8월_9월_10월_11월_12월".split("_"),monthsShort:"1월_2월_3월_4월_5월_6월_7월_8월_9월_10월_11월_12월".split("_"),weekdays:"일요일_월요일_화요일_수요일_목요일_금요일_토요일".split("_"),week ...
...
d,d:Zd,dd:Yd,M:Zd,MM:Yd,y:Zd,yy:Yd},dayOfMonthOrdinalParse:/\d{1,2}\./,ordinal:"%d.",week:{dow:1,doy:4}});
/// moment.js locale configuration
/// locale : Montenegrin [me]
///! author : Miodrag Nikić <miodrag@restartit.me> : https://github.com/miodragnikac
var ph={words:{m:["jedan minut","jednog minuta"],mm:["minut","minuta","minuta"],h:["jedan sat","jednog sata"],hh:["sat","sata","sati"],dd:["dan","dana","dana"],MM:[ ...
:ph.translate,y:"godinu",yy:ph.translate},dayOfMonthOrdinalParse:/\d{1,2}\./,ordinal:"%d.",week:{dow:1,doy:7}});
/// moment.js locale configuration
/// locale : Maori [mi]
///! author : John Corrigan <robbiecloset@gmail.com> : https://github.com/johnideal
a.defineLocale("mi", {months:"Kohi-tāte_Hui-tanguru_Poutū-te-rangi_Paenga-whāwhā_Haratua_Pipiri_Hōngoingoi_Here-turi-kōkā_Mahuru_Whiringa-ā-nuku_Whiringa-ā-rangi_Hakihe ...
"njē vit",yy:"%d vite"},dayOfMonthOrdinalParse:/\d{1,2}\./,ordinal:"%d.",week:{dow:1,doy:4}});
/// moment.js locale configuration
/// locale : Serbian Cyrillic [sr-cyrl]
///! author : Milan Janačković <milanjanackovic@gmail.com> : https://github.com/milan-j
var Nh={words:{m:["један минут","једне минуте"],mm:["минут","минуте","минута"],h:["један сат","једног с ...
ата"],hh:["сат","сата","сати"],dd:["дан","дана","дана"],MM:["месец ...
translate,y:"годину",yy:Nh.translate},dayOfMonthOrdinalParse:/\d{1,2}\./,ordinal:"%d.",week:{dow:1,doy:7}});
/// moment.js locale configuration
/// locale : Serbian [sr]
///! author : Milan Janačković <milanjanackovic@gmail.com> : https://github.com/milan-j

```

25 / 35

```

ата"],hh:["сат","сата","сати"],dd:["дан","дана","дана"],MM:["месец ...
translate,y:"годину",yy:Nh.translate},dayOfMonthOrdinalParse:/\d{1,2}\./,ordinal:"%d.",week:{dow:1,doy:7}});
/// moment.js locale configuration
/// locale : Serbian [sr]
///! author : Milan Janačković <milanjanackovic@gmail.com> : https://github.com/milan-j

```

Impact:

Email addresses discovered within the application can be used by both spam email engines and also brute-force tools. Furthermore, valid email addresses may lead to social engineering attacks.

Mitigate threat:

Use generic email addresses such as contact@ or info@ for general communications and remove user/people-specific email addresses from the website; should this be required, use submission forms for this purpose.

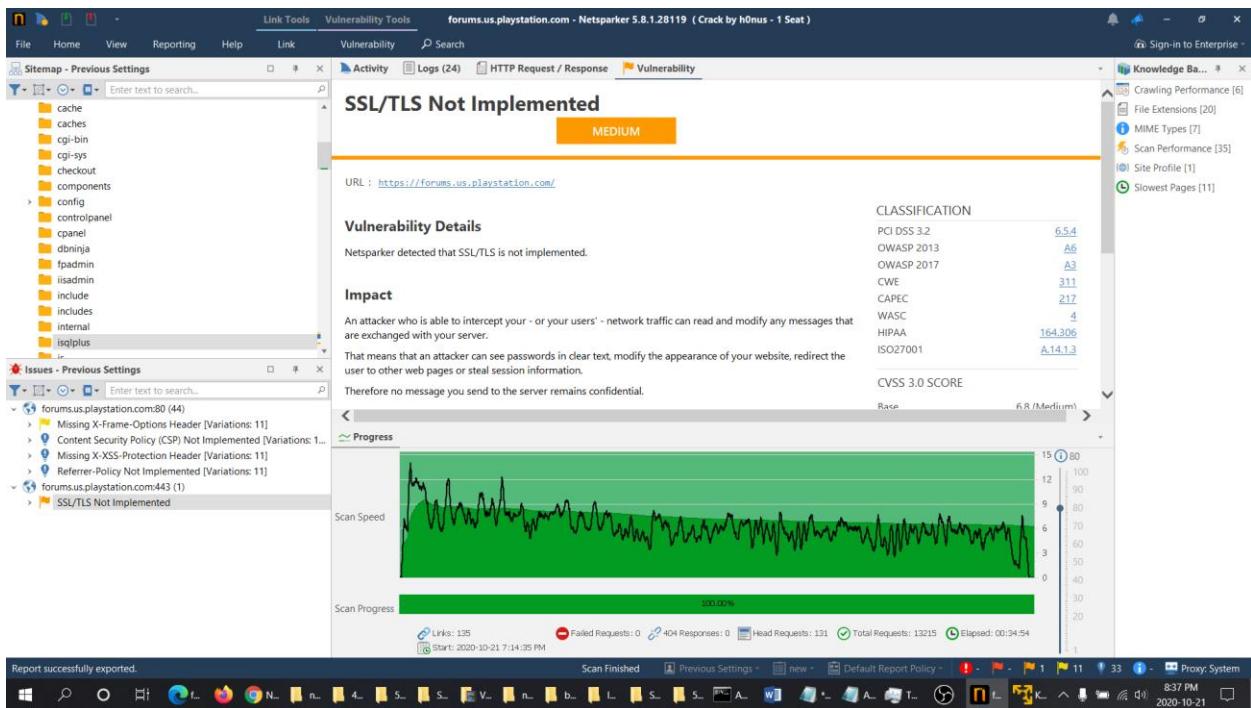
These are the missing headers that should include,

Missing Headers	
Content-Security-Policy	Content Security Policy is an effective measure to protect your site from XSS attacks. By whitelisting sources of approved content, you can prevent the browser from loading malicious assets.
X-Content-Type-Options	X-Content-Type-Options stops a browser from trying to MIME-sniff the content type and forces it to stick with the declared content-type. The only valid value for this header is "X-Content-Type-Options: nosniff".
Referrer-Policy	Referrer Policy is a new header that allows a site to control how much information the browser includes with navigations away from a document and should be set by all sites.
Permissions-Policy	Permissions Policy is a new header that allows a site to control which features and APIs can be used in the browser.

7. <https://forums.us.playstation.com/>

Vulnerability Summary

CONFIRM	VULNERABILITY	METHOD	URL	PARAMETER
	SSL/TLS Not Implemented	GET	https://forums.us.playstation.com/	
	Missing X-Frame-Options Header	GET	http://forums.us.playstation.com/	
	Content Security Policy (CSP) Not Implemented	GET	http://forums.us.playstation.com/	
	Missing X-XSS-Protection Header	GET	http://forums.us.playstation.com/	
	Referrer-Policy Not Implemented	GET	http://forums.us.playstation.com/	



Vulnerability title:

SSL/TLS Not implemented

Risk rating:

Severity: Information

Description:

Netsparker detected that SSL/TLS is not implemented.

Impact:

An attacker who is able to intercept your - or your users' - network traffic can read and modify any messages that are exchanged with your server.

That means that an attacker can see passwords in clear text, modify the appearance of your website, redirect the user to other web pages or steal session information.

Therefore no message you send to the server remains confidential.

Mitigate threat:

We suggest that you implement SSL/TLS properly, for example by using [the Certbot tool](#) provided by the Let's Encrypt certificate authority. It can automatically configure most modern web servers, e.g. Apache and Nginx to use SSL/TLS. Both the tool and the certificates are free and are usually installed within minutes.

8.store.playstation.com

This domain scanned with OWASP ZAP tool and identified some important issues.

The screenshot shows the OWASP ZAP tool interface. At the top, there is a header bar with various menu options like File, Edit, View, Analyse, Report, Tools, Import, Online, Help. Below the header is a toolbar with icons for Quick Start, Request, Response, and other tools. The main window has tabs for Header, Text, Body, and Image. On the left, there is a tree view under 'Contents' and 'Sites'. In the center, there is a preview window showing a screenshot of a game with the title 'SUPER COBRA'. Above the preview, there is a detailed HTTP response header. On the right, a large panel displays an 'Alerts' section. One specific alert is highlighted: 'Cross-Domain Misconfiguration (224)'. This alert is categorized under 'CSP Scanner Wildcard Directive'. The details pane shows the following information:

- URL: https://store.playstation.com/store/api/ichihiro/00_09_000/container/US/en/999/UP0571-CUSA24805_00-HAMPRDC0000000001/1603347032000/image?_version=00_09_000&bg_color=000000&h=124&opacity=100&w=124
- Risk: Medium
- Confidence: Medium
- Parameter:
- Attack:
- Evidence: Access-Control-Allow-Origin: *
- CWE ID: 264
- WASC ID: 14
- Source: Passive (10098 - Cross-Domain Misconfiguration)
- Description: Web browser data loading may be possible, due to a Cross Origin Resource Sharing (CORS) misconfiguration on the web server

At the bottom of the interface, there is a taskbar with various icons and a status bar indicating '252 PM 2020-10-22'.

Vulnerability title:

Cross domain misconfiguration

Risk rating:

Severity:Medium

Description:

Web browser data loading may be possible, due to a Cross Origin Resource Sharing (CORS) misconfiguration on the web server. The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk somewhat

Impact:

This misconfiguration could be used by an attacker to access data that is available in an unauthenticated manner, but which uses some other form of security, such as IP address white-listing.

Mitigate threat:

Ensure that sensitive data is not available in an unauthenticated manner (using IP address white-listing, for instance).

Configure the "Access-Control-Allow-Origin" HTTP header to a more restrictive set of domains, or remove all CORS headers entirely, to allow the web browser to enforce the Same Origin Policy (SOP) in a more restrictive manner.

These are the missing headers that should include,

Missing Headers	
Content-Security-Policy	Content Security Policy is an effective measure to protect your site from XSS attacks. By whitelisting sources of approved content, you can prevent the browser from loading malicious assets.
X-Content-Type-Options	X-Content-Type-Options stops a browser from trying to MIME-sniff the content type and forces it to stick with the declared content-type. The only valid value for this header is "X-Content-Type-Options: nosniff".
Referrer-Policy	Referrer Policy is a new header that allows a site to control how much information the browser includes with navigations away from a document and should be set by all sites.
Permissions-Policy	Permissions Policy is a new header that allows a site to control which features and APIs can be used in the browser.

Reference

- TLS certificate issue-
 - [https://www.cloudinsidr.com/content/known-attack-vectors- against-tls-implementation-vulnerabilities/](https://www.cloudinsidr.com/content/known-attack-vectors-against-tls-implementation-vulnerabilities/)
 - <https://www.helpnetsecurity.com/2014/02/25/identify-and-fix-vulnerabilities-in-your-ssl-certificates/>
- Strict transport security not enforced –
 - https://cheatsheetseries.owasp.org/cheatsheets/HTTP_Strict_Transport_Security_Cheat_Sheet.html
- Security headers-
 - <https://securityheaders.com/>

